**POLITYKA OCHRONY DANYCH OSOBOWYCH**

**(tekst ujednolicony na dzień 19 maja 2022 roku)**

**w organizacji: Nowosądeckie Towarzystwo Pomocy im. św. Brata Alberta   
z siedzibą: 33-300 Nowy Sącz ul. Szwedzka 18, tel. +48 18 443 89 80, +48 18 444 48 10, e-mail: nowysacz@emmaus.pl.**

Na podstawie art. 24 ust. 2, w zw. z art. 5 ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, Dz. Urz. UE L 119 z 04.05.2016 r. z późniejszymi zmianami) Administrator danych osobowych **Nowosądeckie Towarzystwo Pomocy im. św. Brata Alberta** (działający również jako Podmiot Przetwarzający) przyjmuje do stosowania Politykę ochrony danych osobowych.

Informacje (w tym przetwarzane dane osobowe) są bardzo ważnym aktywem Administratora danych, dlatego należy je chronić z należytą starannością, ponieważ wiele procesów i usług zależy w dużej mierze od jakości, poufności, integralności i dostępności informacji. Chroniąc informacje dbamy   
o interesy Administratora danych, jego partnerów i klientów, dlatego bezpieczeństwo informacji ma dla Administratora danych podstawowe znaczenie, aby utrzymać konkurencyjność, ciągłość funkcjonowania, płynność finansową, zgodność z przepisami prawa oraz właściwy wizerunek. Wdrożona u Administratora danych Polityka ochrony danych osobowych (dalej „Polityka”), wraz z dodatkowymi dokumentami, porządkuje kwestie związane z rozliczalnością RODO, zawiera najważniejsze zasady postępowania z informacją oraz wskazuje na szczegółowe instrukcje, procedury i zalecenia związane   
z przetwarzaniem informacji.

Informuję, że w związku z przetwarzaniem danych osobowych u Administratora obowiązują m.in. następujące regulacje:

* Polityka, nazywana również „Polityką ochrony danych osobowych” lub „Polityką bezpieczeństwa danych osobowych”, wraz z instrukcjami, procedurami i wzorami dokumentów,
* Zasady postępowania:
  + „wszystko co nie jest wyraźnie dozwolone jest zabronione”,
  + czystego biurka i czystego ekranu,
  + ograniczonego zaufania w kontaktach wewnątrz oraz poza podmiotem.

**Obowiązkiem każdego pracownika i współpracownika Administratora danych jest przestrzeganie wymienionych zasad oraz postanowień Polityki**.

**§1.**

**DEFINICJE**

1. Na potrzeby niniejszej Polityki, przyjmuje się następujące znaczenie dla poniżej wymienionych sformułowań:

a) „RODO” - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie   
o ochronie danych, Dz. Urz. UE L 119 z 04.05.2016 r. z późniejszymi zmianami);

b) „Administrator” – **Nowosądeckie Towarzystwo Pomocy im. św. Brata Alberta**;

c) „podmiot przetwarzający” - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora;

d) „organ nadzorczy” – Prezes Urzędu Ochrony Danych Osobowych;

e) „podmiot danych” - osoba, której dane osobowe są przetwarzane;

f) „naruszenie ochrony danych osobowych” - naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

g) „Polityka” – Polityka ochrony danych osobowych w organizacji **Nowosądeckie Towarzystwo Pomocy im. św. Brata Alberta**;

*h) „IOD” – Inspektor Ochrony Danych, w przypadku wyznaczenia przez Administratora*.

**§2.**

**OCENA GOTOWOŚCI DO WDROŻENIA RODO**

Administrator przeprowadził ocenę gotowości do wdrożenia i stosowania RODO (ocena stosowanej do 19 maja 2022 r. dokumentacji w zakresie ochrony danych osobowych).

**§3.**

**OGÓLNE ZASADY DOPEŁNIANIA OBOWIĄZKÓW INFORMACYJNYCH**

1. Administrator dopełnienia obowiązków informacyjnych wobec podmiotów danych na zasadach określonych w art. 13 i 14 RODO, z zastrzeżeniem ew. zmian (ograniczeń) wprowadzonych przez krajowe przepisy szczegółowe, wydane na podstawie art. 23 RODO.

2. Wprowadza się wzór klauzul informacyjnych, o których mowa w art. 13 i 14 RODO.

3. Dopełnienie obowiązku informacyjnego, o którym mowa w art. 13 i 14 RODO następuje poprzez wywieszenie klauzuli w siedzibie Administratora, a w razie takiej decyzji Administratora także poprzez zmieszczenie klauzuli informacyjnej na stronie Internetowej Administratora, w treści stosowanych formularzy oraz w stopce korespondencji e-mail. Podczas pozyskiwania danych pracownika, wykonawcy lub wolontariusza Administrator udziela wszelkich informacji, o których mowa w art. 13 RODO.

4. Pracownicy Administratora konsultują treść poszczególnych klauzul informacyjnych z Zarządem i IOD (jeśli wyznaczono).

**§4.**

**WYZNACZENIE INSPEKTORA OCHRONY DANYCH**

Administrator nie wyznacza Inspektora ochrony danych, z uwagi na to, iż nie spełnia żadnej   
z przesłanek, określonych w art. 37 ust. 1 RODO. Administrator nie jest organem lub podmiotem publicznym. Administrator po przeprowadzeniu szczegółowej analizy ustalił, iż główna działalność administratora nie polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę, jak również główna działalność administratora nie polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 RODO oraz danych osobowych, o których mowa w art. 10 RODO.

**§5.**

**ZASADY UPOWAŻNIANIA DO PRZETWARZANIA DANYCH OSOBOWYCH**

1. Administrator podejmuje działania w celu zapewnienia, by każda osoba fizyczna działająca z jego upoważnienia, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na jego polecenie, chyba że wymaga tego od niej prawo Unii lub prawo państwa członkowskiego.

2. Wzór upoważnienia do przetwarzania danych osobowych stanowi ***odrębny dokument***.

3. Wzór rejestru osób upoważnionych do przetwarzania danych osobowych stanowi ***odrębny dokument*** i stosowany jest fakultatywnie, w przypadku decyzji o nadawaniu numerów poszczególnym upoważnieniom.

4. Upoważnienia nadawaną są zgodnie z zasadą minimalizacji danych. Osoba upoważniona przetwarza wyłącznie dane niezbędne do realizacji celów przetwarzania i zgodnie ze swoim zakresem czynności.

**§6.**

**REJESTR CZYNNOŚCI PRZETWARZANIA I KATEGORII CZYNNOŚCI PRZETWARZANIA**

1. Wytyczne w zakresie prowadzenia Rejestru czynności przetwarzania i Rejestru kategorii czynności przetwarzania, będące zaleceniami organu nadzorczego, stanowią ***odrębny dokument***.

2. Wzór Rejestru czynności przetwarzania stanowi ***odrębny dokument (arkusz kalkulacyjny   
z możliwością wydruku)***.

3. Wzór Rejestru kategorii czynności przetwarzania stanowi ***odrębny dokument (arkusz kalkulacyjny z możliwością wydruku)***.

4. Rejestry, o których mowa w ust. 2 i 3 prowadzi Administrator w formie elektronicznej. Zaleca się wydruk i podpis Zarządu w celu zapewnienia autentyczności.

**§7.**

**PRZETWARZANIE NA PODSTAWIE ZGODY**

1. W przypadku, gdy postawą przetwarzania jest zgoda osoby, której dane dotyczą, administrator, działając w celu wykazania, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych, stosuje oświadczenie o wyrażeniu zgody na przetwarzanie danych osobowych,   
w konkretnym celu, złożone świadomie i dobrowolnie. Administrator dokumentuje fakt złożenia oświadczenia pisemnie lub w formie elektronicznej.

2. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie i następuje poprzez dostarczenie oświadczenia w formie pisemnej lub za pośrednictwem poczty e-mail.

3. Od zgody na przetwarzanie danych może być uzależnione wykonanie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej usługi.

**§8.**

**PROCEDURY ŻĄDANIA DOSTĘPU DO DANYCH**

1. Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz uzyskania informacji określonych w art. 15 ROOD. Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, jest informowana o odpowiednich zabezpieczeniach, o których mowa w art. 46 RODO, związanych   
z przekazaniem.

2. Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu, z zastrzeżeniem, iż za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, administrator pobierze opłatę w wysokości wynikającej z kosztów administracyjnych, o czym informuje wnioskodawcę, przed dostarczeniem kopii danych.

3. Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

4. Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, **wyłącznie** na zasadach określonych w art. 17 RODO.

5. Osoba, której dane dotyczą, ma prawo żądania od administratora ograniczenia przetwarzania **jedynie w przypadkach**, o których mowa w art. 18 RODO.

6. Administrator informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, których dokonał zgodnie z art. 16, art. 17 ust. 1 i art. 18 RODO, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

7. Osoba, której dane dotyczą, ma prawo otrzymać od administratora w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe, wyłącznie na warunkach określonych w art. 20 RODO.

8. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e) lub f) RODO, w tym profilowania. Administrator nie będzie przetwarzać tych danych osobowych, chyba że wykaże istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń. Najpóźniej przy okazji pierwszej komunikacji z osobą, której dane dotyczą, wyraźnie informuje się ją o prawie, o którym mowa w art. 21 ust. 1 i 2 RODO oraz przedstawia się je jasno i odrębnie od wszelkich innych informacji.

9. Osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa, na zasadach określonych w art. 22 RODO.

10. Administrator udostępnia osobie, której dane dotyczą, żądane informacje i dane w formie pisemnej lub elektronicznej.

**§9.**

**OCENA PODMIOTU PRZETWARZAJĄCEGO**

1. Jeżeli przetwarzanie ma być dokonywane w imieniu administratora, będzie on korzystał wyłącznie   
z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO   
i chroniło prawa osób, których dane dotyczą.

2. Wzór umowy powierzenia przetwarzania danych osobowych stanowi ***odrębny dokument***.

3. Ocena gwarancji, o których mowa w ust. 1, dokonywana jest poprzez przyjęcie od Podmiotu przetwarzającego oświadczenia, **kwestionariusza** lub poprzez wykonaną przez Administratora inspekcję (stosowanie do ujawnionego ryzyka).

**§10.**

**RETENCJA DANYCH**

1. Dane osobowe będą przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane   
z poszanowaniem norm archiwalnych i przepisów prawa.

2. Okres przechowywania danych osobowych został wskazany przez Administratora w treści prowadzonego przez niego Rejestru czynności przetwarzania oraz zależy od podstawy prawnej przetwarzania i nie może być dłuższy niż wynika to z danej podstawy prawnej. W szczególności dane będą przechowywane:

a) w przypadku przetwarzania danych na podstawie zgody – do momentu wycofania zgody,

b) w przypadku przetwarza danych osobowych na podstawie uzasadnionego interesu Administratora, okres przetwarzania trwa do momentu ustania ww. interesu (np. okres przedawnienia roszczeń cywilnoprawnych) lub do momentu wniesienia sprzeciwu wobec takiego przetwarzania (jeśli dotyczy),

c) w przypadku przetwarza danych osobowych, ponieważ jest to konieczne z uwagi na obowiązujące przepisy prawa – do upływu okresów określonych przez te przepisy (w szczególności przepisy ustawy o rachunkowości, przepisy ustaw podatkowych oraz przepisy ustaw szczegółowych),

d) w przypadku przetwarzania danych na podstawie umowy – do momentu zakończenia obowiązywania umowy, jak również przedawnienia wynikających z niej roszczeń.

3. Po upływie okresu przechowywania danych osobowych Administrator dokona usunięcia danych osobowych oraz usunięcia ich kopii.

**§11.**

**OCENA SKUTKÓW DLA OCHRONY DANYCH**

Ocena skutków dla ochrony danych jest dokonywana na postawie art. 35 RODO.

**§12.**

**UPRZEDNIE KONSULTACJE**

1. Jeżeli ocena skutków dla ochrony danych, o której mowa w art. 35 RODO, wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania administrator konsultuje się z organem nadzorczym.

2. Administrator prowadzi dokumentacje w zakresie realizacji obowiązku wynikającego z art. 35 i 36 RODO.

**§13.**

**KODEKSY POSTĘPOWANIA I MECHANIZMY CERTYFIKACJI**

Nie dotyczy

**§14.**

**PRZEKAZYWANIE DANYCH OSOBOWYCH DO PAŃSTW TRZECICH LUB ORGANIZACJI MIĘDZYNARODOWYCH**

Nie dotyczy

**§15.**

**BEZPIECZEŃSTWO TECHNICZNE I ORGANIZACYJNE**

1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, administrator   
– zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą.

2. Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych

3. Administrator wprowadza środki techniczne i organizacyjne mające zapewnić bezpieczeństwo danych osobowych, określone w rejestrach wydanych na podstawie art. 30 RODO, **w szczególności**:

a) oprogramowane antywirusowe i firewall,

b) szyfrowanie dysków komputerów i pamięci przenośnych lub zabezpieczenie ich hasłem,

c) możliwość zabezpieczania treści wysyłanych wiadomości e-mail za pomocą hasła,

d) składowanie dokumentacji w pomieszczeniach oddzielonych od wspólnej strefy dostępu poprzez drzwi zwykłe zamykane na klucz lub w szafach zamykanych na klucz,

e) dostęp do dokumentacji zawierających dane osobowe tylko przez osoby posiadające aktualne upoważnienia,

f) cykliczne szkolenia pracowników i wykonawców,

g) umowy lub klauzule o poufności,

h) stosowane polityki ochrony danych i wytycznych w zakresie postępowania z danymi,

i) nadzór kierownictwa w ramach struktury,

j) monitoring wizyjny.

4. Osoby upoważnione do przetwarzania danych osobowych:

a) informują administratora o wszelkich zauważonych nieprawidłowościach w działaniu systemu lub przy przetwarzaniu danych osobowych,

b) stosują przyjęte zasady polityki haseł i uwierzytelniania,

c) utrzymują w ścisłej tajemnicy hasła, którymi się posługują,

d) dokonują zmiany hasła w przypadku powzięcia podejrzenia lub stwierdzenia, że z hasłem mogły zapoznać się osoby trzecie,

e) w przypadku odejścia od komputera blokują do niego dostęp za pomocą hasła,

f) ustawiają ekrany komputerów, w taki sposób, aby osoby nieupoważnione nie miały dostępu do ekranów,

g) nie instalują we własnym zakresie nieuprawnionego oprogramowania,

i) informuje niezwłocznie Administratora o podejrzeniu naruszenia ochrony danych,

j) przechowywanie danych osobowych na odpowiednio zabezpieczonych serwerach a nie lokalnie (dotyczy przede wszystkim osób pracujących poza siedzibą organizacji); przechowywanie lokalne tylko za zgodą administratora na nośnikach zabezpieczonych mechanizmem szyfrowania i uwierzytelniania.

5. W zakresie bezpieczeństwa informatycznego i fizycznego:

a) dostęp do baz danych oraz systemów informatycznych przetwarzających dane osobowe mają wyłącznie osoby posiadające stosowne upoważnienia wydane przez Administratora,

b) dostęp do pomieszczeń, w których przetwarzane są dane osobowe, zawarte w zbiorach administrowanych przez ADO, mają: pracownicy i współpracownicy Administratora, posiadający odpowiednie upoważnienie, uprawnione przez Administratora oraz (na mocy umowy powierzenia przetwarzania danych) przez Procesora osoby i pracownicy firm/organizacji współpracujących; przebywanie w tych pomieszczeniach osób niedopuszczonych/nieupoważnionym do przetwarzania danych osobowych może się odbywać tylko w obecności przedstawiciela Administratora lub przedstawiciela Procesora lub osób upoważnionych; w przypadku opuszczenia pomieszczeń (wchodzących w skład obszaru przetwarzania danych osobowych) przez osoby upoważnione, pomieszczenia te zobowiązane są opuścić również osoby nieupoważnione, znajdujące się w tym czasie pod ich nadzorem,

c) drzwi wejściowe do pomieszczeń obszaru przetwarzania danych muszą pozostawać zamknięte zarówno po zakończeniu pracy przez osoby upoważnione, jak i w wypadku każdego, chociażby chwilowego, opuszczenia przez nie pomieszczenia w ciągu czasu pracy; w przypadku opuszczenia pomieszczenia osoba upoważniona zobowiązana jest do zabrania ze sobą klucza do drzwi lub karty dostępu którą dysponuje i zabezpieczenia pomieszczenia przed dostępem osób nieupoważnionych;   
w przypadku utraty klucza lub karty dostępu osoba upoważniona zobowiązana jest do natychmiastowego poinformowania o tym fakcie Administratora.

6. Do przesłanek wskazujących na naruszenie bezpieczeństwa ochrony danych należą m. in.:

* 1. próby błędnych logowań do systemów przetwarzających dane osobowe,
  2. próby nieautoryzowanego dostępu do baz danych,
  3. próby wynoszenia danych na nośnikach pamięci masowych,
  4. pozostawienie wydruków danych osobowych na drukarkach, kserokopiarkach lub innych urządzeniach poligraficznych lub w miejscach niechronionych,
  5. wysyłanie, przez osoby nieupoważnione, dokumentów lub informacji zawierających dane osobowe za pośrednictwem poczty elektronicznej lub konwencjonalnej oraz urządzeń teletransmisyjnych.

**§16.**

**WYKORZYSTYWANIE PRYWATNYCH URZĄDZEŃ PRACOWNIKÓW DO CELÓW SŁUŻBOWYCH**

1. Wykorzystywanie prywatnych urządzeń pracowników administratora do celów służbowych jest dopuszczalne wyłącznie po uzyskaniu pisemnej zgody administratora i określeniu zasada takiego postępowania.

2. Pracownik, który wykorzystuje prywatne urządzenie do celów służbowych, wyraża zgodę na dostęp upoważnionego pracownika administratora do zasobów jego urządzenia w celu zabezpieczenia danych będących własnością administratora lub ich usunięcia.

3. Administrator indywidualnie, wobec każdego z pracowników i w formie pisemnej, ustala zasady dotyczące wykorzystania urządzeń mobilnych i/lub pracy w systemie zadaniowego czasu pracy (w tym zdalnie lub w terenie), tak aby zapewnić bezpieczeństwo informacji i ochrony danych.

**§17.**

**POLITYKA CZYSTEGO BIURKA I EKRANU**

Administrator zobowiązuje wykonawców i pracowników upoważnionych do przetwarzania danych osobowych, do zachowania polityki czystego biurka, czystego ekranu i czystych tablic.

**§18.**

**AUDYT WEWNĘTRZNY**

1. Administrator prowadzi regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych. Administrator ocenia stosowane mechanizmy szyfrowania i pseudonimizacji, jak również ocenia możliwość stosowania tego typu zabezpieczeń w poszczególnych procesach firmy. Administrator zapewnia zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania, jak również zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

2. Administrator monitoruje przestrzegania RODO oraz niniejszej polityki.

3. Administrator nie rzadziej niż raz na rok prowadza audyty wewnętrzny, mające na celu ocenę zgodności przetwarzania danych z RODO lub zleca niezależnemu podmiotowi przeprowadzenie audytu zewnętrznego. Podczas audytów badane są w szczególności obszary, o których mowa w ust. 1.

**§19.**

**PROCEDURA POSTĘPOWANIA W RAZIE NARUSZENIA ORAZ PROCEDURA POWIADOMIENIA O NARUSZENIU DANYCH**

1. W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55 RODO, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

2. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi, zgodnie z postanowieniami umowy o powierzenie przetwarzania danych osobowych, zawartej z podmiotem przetwarzającym.

3. Zgłoszenie dokonywane jest w formie przyjętej przez organ nadzorczy. Treść zgłoszenia zawiera elementy wskazane w art. 33 ust. 3 RODO.

4. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze oraz prowadzi rejestr naruszeń.

5. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą,   
o takim naruszeniu. Zawiadomienie ma formę pisemną. Zawiadomienie nie jest wymagane w sytuacjach wskazanych w art. 34 ust. 3 RODO.

**§20.**

**DZIAŁANIA SZKOLENIOWE I UŚWIADAMIAJĄCE**

1. Administrator wprowadza następujące zasady realizacji działań szkoleniowych: szkolenia dla osób upoważnionych raz w roku oraz szkolenie każdej nowo upoważnionej osoby.

2. Administrator wprowadza następujące zasady realizacji działań upowszechniających: biuletyn informacyjne raz na kwartał.

**§21.**

**METODYKA ZARZĄDZANIA RYZYKIEM**

Zawarto w **odrębnym dokumencie**.

*Odrębne dokumenty, wprowadzone i zakomunikowane przez Administratora, w zakresie sposobów przetwarzania i ochrony danych osobowych stają się integralną częścią niniejszej Polityki*.

19.04.2022 r.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Data i podpis administratora danych